

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ALI AL-AHMED,
Plaintiff,
v.
TWITTER, INC., et al.,
Defendants.

Case No. [21-cv-08017-EMC](#)

**ORDER GRANTING DEFENDANT'S
MOTION TO DISMISS**

Docket No. 30

I. INTRODUCTION

Plaintiff Al-Ahmed is a critic of the Kingdom of Saudi Arabia (“KSA”) and has been granted asylum in the United States. Between 2013–2015, two of Twitter’s (now former) employees, Defendants Ahmad Abouammo and Ali Hamad A. Alzabarah, accessed user information on Al-Ahmed without authorization and provided it to KSA government officials. Al-Ahmed filed this lawsuit against Abouammo, Alzabarah, and Twitter for violating the Electronics Communications Privacy Act (“EPCA”), violating the Computer Fraud and Abuse Act (“CFAA”), violating the Stored Communications Act (“SCA”), violating California’s Unfair Competition Law (“UCL”), breach of contract, intrusion upon seclusion, unjust enrichment, promissory estoppel, negligence, negligent hiring, supervision, and retention, civil conspiracy, and replevin. Al-Ahmed alleges that his Twitter account was hacked, which led to the KSA targeting him and those around him. Furthermore, he alleges that Twitter’s suspension of his account in 2018 punishes him—the victim—and ratifies its former employees’ conduct. Pending in this Court is Twitter’s motion to dismiss Al-Ahmed’s Complaint. The Court **GRANTS** Twitter’s motion for the reasons stated below.

II. BACKGROUND

Al-Ahmed alleges as follows in the Complaint:

Al-Ahmed is one of the leading critics of the KSA who resides and has been granted asylum in the United States. Docket No. 1 (“Complaint”) at 2. Between August 2013 and December 2015, Twitter user information was accessed without authorization and provided to KSA government officials, which Twitter failed to detect for a period of time spanning over a year. *Id.* at 4, 7. Al-Ahmed’s Arabic Twitter account, which has over 36,000 followers worldwide, was one of the accounts breached during this time. *Id.* at 6. Al-Ahmed contends that his private information, including his personal phone number and email address, which he never made publicly available, was compromised due to Twitter’s conduct. *Id.* at 16. His account also had confidential information provided by his followers and journalistic sources. *Id.* at 3. Al-Ahmed alleges his private information was used by the KSA to silence him by stripping him of his Saudi nationality, keeping him under surveillance, and attempting to kidnap and kill him on multiple occasions. *Id.* at 6–7. His followers on Twitter, or those who otherwise contacted him using Twitter, have disappeared, been arrested, or have been executed. *Id.* at 8. According to him, “the KSA managed to fully silence [him] when they . . . suspend[ed his] Arabic Twitter account, without explanation, warning, or justification.” *Id.* at 8.

On November 19, 2019, Abouammo and Alzabarah were indicted for acting as agents for the government of Saudi Arabia while employed at Twitter. *Id.* at 4. Abouammo was the Media Partnerships Manager responsible for the Middle East and North Africa region at Twitter. *Id.* at 3. Alzabarah was a Site Reliability Engineer whose responsibility was maintaining Twitter’s hardware and software to ensure uninterrupted service. *Id.*

A. Twitter’s Notice

On or about December 11, 2015, Twitter sent the following notice to a small group of its users:

Dear @{{screen_name}}, As a precaution, we are alerting you that **your Twitter account is one of a small group of accounts that may have been targeted by state-sponsored actors. We believe that these actors (possibly associated with a government) may have been trying to obtain information such as email addresses,**

IP addresses, and/or phone numbers.

At this time, we have no evidence they obtained your account information, but we're actively investigating this matter. We wish we had more we could share, but we don't have any additional information we can provide at this time.

It's possible your account may not have been an intended target of the suspected activity, but we wanted to alert you as soon as possible. We recognize that this may be of particular concern if you choose to Tweet using a pseudonym. For tips on protecting your identity online, you may want to visit the Tor Project or EFF's Protecting Yourself on Social Networks.

Id. at 14. Al-Ahmed alleges that this notice was insufficient because it failed to indicate that these state-sponsored actors committed these data breaches while they were located on Twitter's premises, employed by Twitter, using Twitter's resources, at the direction of Twitter. *Id.* at 15.

B. Twitter's Actions in Aid of the KSA

Al-Ahmed alleges that Twitter provided the two employees with access to Twitter's resources with the full knowledge that they were improperly accessing user data, helped them provide the information to the KSA, and helped them cover up their tracks by purging its internal database of incriminating evidence. *Id.* at 7. Al-Ahmed also alleges that Twitter's Privacy Policy suggests that Tweets may be protected by opting to allow only Twitter followers to see them through account settings, which created an illusion of security and safety. *Id.* at 10. Al-Ahmed lastly alleges that Twitter failed to safeguard user data, evidenced by its disclosure to the Securities and Exchange Commission in 2020. The disclosure stated that Twitter received a draft complaint from the Federal Trade Commission alleging "violations...[r]elate[d] to the Company's use of phone number and/or email address data provided for safety and security purposes [ostensibly for targeted advertising] during periods between 2013 and 2019." *Id.* at 12. Thus, Twitter negligently failed to implement policies, practices, and safeguards that would have prevented the acts of its former employees. *Id.* at 37.

C. Twitter's Relationship with the KSA

In 2011, Saudi Prince Alwaleed Bin Talal purchased \$300 million worth of stock in Twitter. *Id.* In 2015, Bin Talal made an additional investment, owning 5.2% of the company, more than Twitter's founder and CEO. *Id.* at 2. Bin Talal later signed over many of his assets to

Crown Prince Bin Salman. *Id.* Thus, Al-Ahmed alleges that Twitter’s acts were designed to appease Bin Salman, a significant investor. *Id.* According to Al-Ahmed, Bader al-Asaker is the head of Bin Salman’s affairs and the “Saudi mastermind” behind the Twitter spy scandal. *Id.* at 13. He claims that Asaker is “Foreign Official-1” in the United States Attorneys Offices’ indictment against Abouammo and Alzabarah. *Id.* Al-Ahmed alleges that Asaker provided Abouammo and Alzabarah with “gifts, cash payments, and promises of future employment in exchange for nonpublic information about Twitter uses, which constituted valuable property...” *Id.* Furthermore, Twitter CEO Jack Dorsey met with both Asaker and Bin Salman at Twitter’s headquarters on June 25, 2016, and at least one additional time in Riyadh thereafter. *Id.* at 13. Dorsey and Asaker follow each other on Twitter. *Id.*

D. Twitter’s Suspension of Al-Ahmed’s Account

In 2018, Al-Ahmed’s Twitter account was suspended, preventing access to his followers. *Id.* at 8. Al-Ahmed alleges that, as a result, he lost significant revenue and earning potential related to his work as a journalist, as much of his work was contingent on his online presence. *Id.* at 16. Al-Ahmed further alleges that his appeal of the suspension failed despite Alzabarah and Abouammo’s indictment. *Id.* at 8. According to Al-Ahmed, preventing access to his account and the list of his followers, punishes the victim and “ratifie[s] the actions of its supposedly errant employees and show[s] [Twitter’s] continuing allegiance to the KSA.” *Id.*

III. LEGAL STANDARD

A. Motion to Dismiss

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Fed. R. Civ. P. 12(b)(6) motion to dismiss after the Supreme Court’s decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) and *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), a plaintiff’s “factual allegations [in the complaint] ‘must . . . suggest that the claim has at least a plausible chance of success.’” *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court “accept[s] factual allegations in the complaint as true and

1 construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St.*
 2 *Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But “allegations in a
 3 complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient
 4 allegations of underlying facts to give fair notice and to enable the opposing party to defend itself
 5 effectively.” *Levitt*, 765 F.3d at 1135 (quoting *Eclectic Props. E., LLC v. Marcus & Millichap*
 6 *Co.*, 751 F.3d 990, 996 (9th Cir. 2014)). “A claim has facial plausibility when the Plaintiff pleads
 7 factual content that allows the court to draw the reasonable inference that the Defendant is liable
 8 for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “The plausibility standard is not akin to a
 9 ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted
 10 unlawfully.” *Id.* (quoting *Twombly*, 550 U.S. at 556).

11 B. Judicial Notice

12 Under Federal Rule of Evidence 201, “[a] judicially noticed fact must be one not subject to
 13 reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the
 14 trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy
 15 cannot reasonably be questioned.” Fed. R. Evid. 201. Courts may take judicial notice of
 16 “undisputed matters of public record,” but generally may not take judicial notice of “disputed facts
 17 stated in public records.” *Lee v. City of Los Angeles*, 250 F.3d 668, 690 (9th Cir. 2001). Facts
 18 subject to judicial notice may be considered on a motion to dismiss. *Mullis v. U.S. Bankr. Ct.*, 828
 19 F.2d 1385, 1388 (9th Cir. 1987). “Proper subjects of judicial notice when ruling on a motion to
 20 dismiss include . . . publically accessible websites[.]” *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d
 21 1190, 1204 (N.D. Cal. 2014) (citing *Caldwell v. Caldwell*, No. 05–4166, 2006 WL 618511, at *4
 22 (N.D. Cal. Mar. 13, 2006); *Wible v. Aetna Life Ins. Co.*, 375 F.Supp.2d 956, 965–66 (C.D.
 23 Cal.2005).

24 The doctrine of incorporation by reference is distinct from judicial notice. The doctrine
 25 “permits a district court to consider documents ‘whose contents are alleged in a complaint and
 26 whose authenticity no party questions, but which are not physically attached to the . . .
 27 pleadings.’” *In re Silicon Graphics Sec. Litig.*, 183 F.3d 970, 986 (9th Cir. 1999) (quoting *Branch*
 28 *v. Tunnell*, 14 F.3d 449, 454 (9th Cir.1994)). The court may incorporate such a document “if the

plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). The Ninth Circuit in *Kniesel* extended this doctrine to apply in some circumstances where the plaintiff does not explicitly allege the contents of the document in the complaint, but the defendant was allowed to attach the document in its motion to dismiss. In order for this extension to apply, the plaintiff's claim must depend on the contents of the document and the parties must not dispute the authenticity of the document. *Kniesel v. ESPN*, 393 F.3d 1068 (9th Cir. 2005) (allowing the introduction of a website's contents that were seen alongside the disputed contents in a defamation suit that were not disputed for authenticity).

Therefore, the requirements for the documents that are relied on by the complaint to be incorporated is that: "(1) the complaint refers to the document; (2) the document is central to the plaintiff's claim; and (3) no party questions the authenticity of the copy attached to the 12(b)(6) motion." *Marder v. Lopez*, 450 F.3d 445, 448 (9th Cir. 2006) (internal citations omitted). Such documents may be considered as "part of the complaint," without converting the Rule 12(b)(6) motion into one for summary judgment. *Ritchie*, 342 F.3d at 908. The contents of such documents may be assumed to be true for purposes of deciding a Rule 12(b)(6) motion. *Id.*

IV. DISCUSSION

A. Twitter's Request for Incorporation by Reference/Judicial Notice

Twitter requests the Court to incorporate by reference or judicially notice the following documents:

- a. Twitter's December 11, 2015 email and in-app notices. Docket No. 29-5 ("Srinivasan Declaration"), Ex. A ("Twitter Employee Declaration"), Ex. 1–2.
- b. Twitter's records reflecting that the December 11, 2015 email notice and in-app notice were sent to Al-Ahmed. Twitter Employee Declaration, Ex. 3–4.
- c. A Twitter message sent by Al-Ahmed through his Twitter account, and a certified English translation of that message. Twitter Employee Declaration, Ex. 5.
- d. A screenshot of Al-Ahmed's active Twitter account. Srinivasan Declaration, Ex.

B.

e. A publicly available Twitter post made by Ali Al-Ahmed that lists his phone number. Srinivasan Declaration, Ex. C.

f. A publicly available press release listing Al-Ahmed's phone number and email address. Srinivasan Declaration, Ex. D.

g. Twitter's current and prior terms of service. Srinivasan Declaration, Ex. E; Twitter Employee Declaration, Ex. 6A–6N.

Al-Ahmed does not directly respond to Twitter's request for incorporation by reference and judicial notice.

1. Incorporation by Reference

Twitter seeks to incorporate by reference five exhibits. *See* Docket No. 31. Exhibits 1 and 2 are notifications Twitter sent to potentially affected Twitter users regarding the unauthorized access of Twitter accounts. *Id.* at 4. Exhibits 1 and 2 may be incorporated by reference because they are referenced extensively in the Complaint and are integral to Al-Ahmed's claims. *Ritchie*, 342 F.3d at 908 ("Even if a document is not attached to a complaint, it may be incorporated by reference into a complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim."). The Complaint directly quotes the contents of these notifications and argues their sufficiency. Docket No. 31 at 5. *See, e.g.*, Complaint at 14, 15; *Daniels-Hall v. National Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010) ("Plaintiff directly quoted the material . . . thereby incorporating [the material] into the Complaint.").

Exhibits 3 and 4 are files maintained in Twitter's records that identify the user accounts that received the notifications. Docket No. 31 at 5. The Complaint does not discuss Al-Ahmed's dispute that he received notice in the Complaint. However, the issue is somewhat hinted at, as Al-Ahmed alleges that "Twitter purportedly sent a notice[.]" Complaint at 14. Al-Ahmed does not dispute that Twitter sent these notices to some people, but disputes that he received notice from Twitter in his Opposition. Opp'n at 4–5, Ex. A at 2. Twitter argues that "where a plaintiff claims he or she never received a notification, and the defendant provides evidence that the defendant did in fact notify the plaintiff, defendant's evidence may be incorporated by reference to prevent the plaintiff from deliberately omitting or contradicting by bald allegation the records reflecting this

information.” *See* Docket No. 38 (“Reply”) at 4–5. These notification lists may be incorporated by reference because “the notifications submitted by [Twitter] are crucial to [Al-Ahmed’s] claims that [he] never received notifications . . . [Al-Ahmed], again, do not raise in [his] Opposition any dispute as to the authenticity of these notifications.” *Starks v. Geico Indem. Co.*, No. CV-15-5771-MWF (PJW), 2015 WL 12942282, at *2 (C.D. Cal. Nov. 10, 2015) (incorporating by reference the notifications allegedly not received by the plaintiff). Accordingly, these exhibits may be treated as part of the Complaint under the incorporation by reference doctrine.

Exhibit 5 consists of an Arabic message transmitted by Al-Ahmed from his Twitter account as well as an English translation of the message. *Id.* at 16. Twitter claims that this message contained hateful and abusive language. *Id.* at 6–7. Twitter argues that this message led to the suspension of Al-Ahmed’s Twitter account and is thus integral to his Complaint. *Id.* However, the Complaint makes no reference to this message and Al-Ahmed’s claims are not dependent on the existence of this message. Although Twitter cites two cases for the proposition that Al-Ahmed is not allowed to plead around the very message he wrote that led to his suspension, these cases are distinguishable.

Twitter first cites *Chyba v. Green Tree Servicing, LLC.*, in which the plaintiff alleged that a loan service provider failed to provide her with written notices related to her loan. No. 12-CV-2530-H (WMC), 2012 WL 12874929, at *1–*2 (S.D. Cal. Dec. 12, 2012). The defendant submitted written correspondences regarding the validation and collection of the debt. *Id.* The court incorporated the letter because “[a]lthough not specifically referenced in her complaint, Plaintiff’s claims depend on this written correspondence.” *Id.* at *2–*3. Here, Al-Ahmed’s claims do not depend on Exhibit 5. This allegedly hateful message is integral not to Al-Ahmed’s allegations but to Twitter’s defense of them. *See Jones v. Raymer Metals, Inc.*, No. CV-17-00546-BROMRWX, 2017 WL 10560488, at *4 (C.D. Cal. May 31, 2017) (distinguishing *Chyba* because while “[w]ritten correspondence between parties” may be considered under the incorporation by reference doctrine . . . Plaintiff does not appear to rely on Defendant’s letter as a basis for her claims.”).

Next, Al-Ahmed cites *Knieval* to argue that exhibits that provide context may be

incorporated by reference. *Id.* (citing *Knievel*, 393 F.3d at 1076). In *Knievel*, the plaintiffs alleged that a photograph and associated caption published on the defendant’s website were defamatory. *Knievel*, 393 F.3d at 1070. The plaintiff attached a photograph of the webpage to the complaint but omitted surrounding web pages that gave context to the photograph. *Id.* at 1076. The Ninth Circuit incorporated by reference the surrounding pages because “a viewer accessing the *Knievel* photograph must also access the surrounding pages” and a court must also take into account “all parts of the communication that are ordinarily heard or read with [a statement].” *Id.* Here, there is no issue with the completeness of an otherwise admissible document. It is a new document altogether.

In addition, Exhibit 5’s authenticity seems to be disputed by Al-Ahmed. Al-Ahmed states in his declaration that he does not recognize this statement in Exhibit 5 and that it is not his statement. Docket No. 32 (“Opp’n”), Exhibit A, at 3. Al-Ahmed also states that its translation is “entirely inaccurate.” *Id.* Documents under dispute cannot be incorporated by reference. *See Knievel*, 393 F.3d at 1068. Accordingly, Exhibit 5 may not be incorporated by reference.

For the foregoing reasons, the Court **GRANTS** Twitter’s motion to incorporate by reference Exhibit 1 and 2 but **DENIES** the motion for Exhibits 3–5.

2. Judicial Notice of Public Documents

Twitter also asks the Court to judicially notice publicly available documents. Exhibits B, C, and D to the Srinivasan Declaration are copies of the landing page of Al-Ahmed’s Twitter account, a public post on the account, and a press release page, which are all available publicly. “Because the exhibits Plaintiff seeks to have judicially noticed are publicly accessible webpages and Defendant does not oppose authentication of the websites[,]” these exhibits are properly subject to judicial notice. *Lindora, LLC v. Limitless Longevity LLC*, No. 15-CV-2847-JAH (KSC), 2016 WL 6804443, at *3 (S.D. Cal. Sept. 29, 2016); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1204 (N.D. Cal. 2014) (noting that publicly accessible websites are subject to judicial notice).

Similarly, Exhibit E to the Srinivasan Declaration and Exhibits 6A–6N to the Twitter Employee Declaration are Twitter’s terms of service (“TOS”) in effect from September 2009 to

the present, and also publicly available on Twitter’s webpage. Accordingly, they also are properly subject to judicial notice. *See Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1068-1069 n.3 (N.D. Cal. 2016) (taking judicial notice of Yelp’s privacy policies); *Datel Holdings Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d 974, 983–84 (N.D. Cal. 2010) (taking judicial notice of Xbox software license and terms of service). Accordingly, the Court **GRANTS** Twitter’s motion to judicially notice Exhibits B, C, D, and 6A–6N.¹

B. The Abdulaziz Case

Throughout the motion, Twitter cites a case with substantially similar facts and allegations that was filed in this district and dismissed three times. *See generally Abdulaziz v. Twitter, Inc.*, 2020 WL 6947929 (Aug. 12, 2020) (“*Abdulaziz I*”); *Abdulaziz v. Twitter, Inc.*, No. 19-CV-06694-LB, 2021 WL 633812, at *7 (N.D. Cal. Feb. 18, 2021) (“*Abdulaziz II*”); *Abdulaziz v. Twitter, Inc.*, No. 19-CV-06694-LB, 2021 WL 2986400, at *1 (N.D. Cal. July 15, 2021) (“*Abdulaziz III*”). This case was brought by another Saudi dissenter and pertains to the same 2013–2015 hacking of the Twitter accounts by the same employees. The plaintiff had alleged that after his Twitter data was hacked, Saudi agents used malware to hack his phone and then targeted his family. *Id.* The plaintiff similarly alleged violations of the SCA, California’s UCL, invasion of privacy, misrepresentation, negligence, and negligent hiring, supervision, or retention of employees. *See Abdulaziz I*, 2020 WL 6947929, *1. *Abdulaziz I* found that the plaintiff lacked Article III standing because he failed to show how the compromise of the Twitter data caused the harm to his family and friends, especially when he was already an outspoken dissident who suffered persecution prior to the hacking of his Twitter account. *Id.* at *6. The court also found that Twitter’s December 2015 notice barred the plaintiff’s claims due to the statute of limitations and defeated any claim that Twitter ratified its employee’s conduct. *Id.* at *7.

In *Abdulaziz II*, the plaintiff alleged negligent supervision and retention of its employees and negligence. The court again held that the plaintiff lacked standing due to lack of causation

¹ Al-Ahmed refers to Exhibit C as a private message in relation to his Privacy Act claim in the Complaint. Nevertheless, this is irrelevant to the judicial notice question because the purported “private message” is publicly available.

1 and that the December 2015 notice was sufficient notice to trigger the statute of limitations under
 2 California’s discovery rule. 2021 WL 633812, at *7. In *Abdulaziz III*, the court dismissed the
 3 case with prejudice for lack of causation required for Article III standing. 2021 WL 2986400, at
 4 *3. Twitter largely relies on this case to argue that Al-Ahmed lacks standing and that the statute
 5 of limitations period has passed.

6 C. Article III Standing

7 Under Rule 12(b)(1), a party may move to dismiss for lack of subject matter jurisdiction.
 8 “[L]ack of Article III standing requires dismissal for lack of subject matter jurisdiction under
 9 [Rule] 12(b)(1).” *Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). The “irreducible
 10 constitutional minimum” of standing requires that a “plaintiff must have (1) suffered an injury in
 11 fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to
 12 be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547
 13 (2016). These three elements are referred to as, respectively, injury in fact, causation, and
 14 redressability. *Planned Parenthood of Greater Was. & N. Idaho v. U.S. Dep’t of Health & Human*
 15 *Servs.*, 946 F.3d 1100, 1108 (9th Cir. 2020). The alleged injury in fact must be “concrete,
 16 particularized, and actual or imminent.” *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203, 210
 17 L. Ed. 2d 568 (2021). “For an injury to be ‘particularized,’ it must affect the plaintiff in a personal
 18 and individual way” and “[o]nly those plaintiffs who have been concretely harmed by a
 19 defendant’s statutory violation may sue that private defendant over that violation in federal court.”
 20 *Spokeo*, 136 S. Ct. at 1548 (internal quotation marks omitted); *Ramirez*, 141 S. Ct. at 2205. “The
 21 plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these
 22 elements[.]” *Spokeo*, 136 S. Ct. at 1547 (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

23 Here, Al-Ahmed’s claims arise from two separate events: (1) the former Twitter
 24 employees’ unauthorized access into Twitter accounts at the behest of the KSA between 2013–
 25 2015, and (2) the May 2018 suspension of Al-Ahmed’s Arabic Twitter account. Docket No. 30
 26 (“Mot.”) at 8. Twitter argues that Al-Ahmed lacks Article III standing relating to the KSA’s 2013
 27 to 2015 espionage, and therefore all claims against Twitter except Replevin must be dismissed.
 28 *Id.*

Twitter argues that Al-Ahmed’s claims do not have Article III standing for the same reason articulated by the *Abdulaziz* courts—he fails to establish a causal nexus between Twitter’s actions and the injury, and any such injury is not particularized to Al-Ahmed. *Id.* at 10. Al-Ahmed argues that: (1) an injury exists solely by virtue of statutes creating legal rights; (2) Twitter’s invasion of his privacy is a harm in itself; and (3) that he has nevertheless alleged a concrete and particularized injury apart from the invasion to his privacy. Opp’n at 3 (citing *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982) (internal quotations omitted)). Al-Ahmed’s first and third arguments fail. However, invasion of privacy is a particularized injury sufficient to establish Article III standing.

The first argument fails because this argument was explicitly rejected by the Supreme Court in 2016. *Spokeo*, 136 S. Ct. at 1543 (“Article III standing requires a concrete injury even in the context of a statutory violation.”). The third argument also fails because Al-Ahmed fails to identify a concrete and personal injury separate from the invasion of privacy itself. Although Al-Ahmed’s affidavit to his Opposition states: “as a freelance journalist and author this has cost me hundreds of thousands of dollars in lost revenue from writing articles and books and through podcasts[,]” this injury is not alleged in his Complaint. Opp’n, Ex. A; *Remington v. Mathson*, 42 F. Supp. 3d 1256, 1278 n.3 (N.D. Cal. 2012), *aff’d*, 575 F. App’x 808 (9th Cir. 2014) (“A Complaint cannot be amended through allegations made in an opposition to a motion to dismiss.”); *Schneider v. California Dep’t of Corr.*, 151 F.3d 1194, 1197 n.1 (9th Cir. 1998) (“In determining the propriety of a Rule 12(b)(6) dismissal, a court may not look beyond the complaint to a plaintiff’s moving papers, such as a memorandum in opposition to a defendant’s motion to dismiss.”). Even if this statement is taken into consideration, it fails to establish standing because it lacks any causal connection to the alleged KSA-sponsored espionage claims. The preceding paragraph to this sentence makes clear that it was Twitter’s suspension of his account in 2018 that prevented him “from accessing the tens or thousands of KSA and other Arab-language followers and sources [that] curtailed [his] ability to report credibly and in real time on events unfolding in the KSA [and cost him his revenue.]” Docket No. 32-1, Ex. A at 5–6. The hacking of his account is distinct from the termination of his account.

Nevertheless, invasion of privacy by itself is sufficiently concrete and particularized to confer Article III standing. Last year, the Supreme Court further clarified the scope of Article III standing that: “Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion.” *Ramirez*, 141 S. Ct. at 2204.

In the years between *Spokeo* and *Ramirez*, the Ninth Circuit found Article III standing in multiple privacy-related claims such as ECPA and SCA claims. *See Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020). The Ninth Circuit explained:

the legislative history and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA. *See* S. REP. NO. 99-541, at 2 (1986) (“[The Wiretap Act] is the primary law protecting the security and privacy of business and personal communications in the United States today.”); *Id.* at 3 (“[The SCA] is modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. to protect privacy interests in personal and proprietary information”); Cal. Pen. Code § 630 (noting that CIPA was passed “to protect the right of privacy of the people of this state”). Thus, these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing.

In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 599 (9th Cir. 2020) (finding standing to pursue privacy claims under the Wiretap Act, SCA, and CIPA because Facebook’s tracking and collection of personal information would constitute “harm to their interest in controlling their personal information”). Therefore, an invasion of privacy as a harm is sufficient here. *See Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (“Privacy torts do not always require additional consequences to be actionable . . . the ‘intrusion itself’ makes the defendant liable.” (citing Restatement (Second) of Torts § 652B cmt. b. (Am. Law Inst. 1977))); *Lynch v. AML Network Ltd.*, No. CV 21-3574-GW-RAOX, 2021 WL 4453470, at *3 (C.D. Cal. Sept. 27, 2021) (“The Ninth Circuit has expressly held that “a violation of the TCPA is a concrete, de facto injury.”).

The disclosure of Al-Ahmed’s private information, including his personal phone number and email address would similarly constitute “harm to [his] interest in controlling [his] personal

information” and is a violation of a statutory right to privacy. *In re Facebook*, 956 F.3d at 599; *see also Eichenberger*, 876 F.3d at 983 (finding that the VPPA identifies a substantive right to privacy against a disclosure of an individual’s personally identifiable information). Accordingly, Al-Ahmed’s injury is sufficiently concrete and particularized.

Twitter argues that Al-Ahmed fails to establish that his alleged injury is “fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.” Reply at 2 (citing *Lujan*, 504 U.S. at 560–61). To the extent that Al-Ahmed alleges that these breaches of privacy caused other harms such as the disappearance, arrest, or execution of his followers, his claims fail because he “does not explain how the compromise of the Twitter data caused the harm[.]” *Abdulaziz I*, 2020 WL 6947929, at *6. Any harm to Al-Ahmed, if alleged to be a result of the harm or disappearance of his followers, cannot be established due to lack of causation. Al-Ahmed fails to allege that his followers were harmed by the breach of privacy. Merely alleging harm to “several” Twitter users who either followed him on Twitter or have messaged him, out of the 36,000 followers that he had, is insufficient. Indeed, the only specific example Al-Ahmed points to is a follower of his Twitter account who was also a Saudi Dissident. Complaint at 8. The article cited by Al-Ahmed describes him as “one of the kingdom’s most prominent and persistent dissidents” who had “frequent prison terms.” *Id.* at 8, n.8. As such, Al-Ahmed fails to plead any facts that would suggest that the breach of privacy led to his imprisonment and death.

On the other hand, Al-Ahmed alleges unauthorized access of his Twitter account resulted in harm to him described above is traceable to Abouammo and Alzabarah who were Twitter employees. Al-Ahmed’s theory against Twitter is one of vicarious liability for its employees’ conduct. Accordingly, this conduct is “fairly traceable” to Twitter.

For the foregoing reasons, Al-Ahmed has Article III standing.

D. Statute of Limitations

1. *Abdulaziz I and II*

The statute of limitations issue here concerns the same December 2015 notice discussed in *Abdulaziz I and II*. The *Abdulaziz I* court held that this December 2015 notice barred most of

plaintiff's claims, including the negligence and negligent hiring claims. *Abdulaziz I*, 2020 WL 6947929, at *7; *Abdulaziz II*, 2021 WL 633812, at *7. Under the same reasoning, Twitter argues that Al-Ahmed's claims accrued when he received the 2015 notices alerting him that his account information had been exposed. Mot. at 12. Since the Complaint was filed on October 13, 2021, more than 5 years have passed since the notice of the unauthorized intrusion of his Twitter account, and more than 3 years have passed since the suspension of his account.² Therefore, Twitter contends that all of Al-Ahmed's claims, except his breach of contract and civil conspiracy claims (to the extent they are premised on his account suspension) are time-barred. *Id.* Al-Ahmed argues that he is saved from the time ban by California's discovery rule; he contends his claims did not accrue until the Twitter employees' indictment in 2019. Opp'n at 5.

2. Notice and the Discovery Rule

a. The Delayed Discovery Rule

Pursuant to the "discovery rule," the accrual of a cause of action is postponed until the "plaintiff discovers, or has reason to discover, the cause of action." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 807, 110 P.3d 914, 920 (2005). "A plaintiff has reason to discover a cause of action when he or she has reason at least to suspect a factual basis for its elements." *Id.* Therefore, it is inquiry notice, not actual notice, that is relevant to the discovery rule. *Id.* For the

² The ECPA, CFAA, SCA, promissory estoppel, intrusion upon seclusion, negligent hiring, and negligence claims each have two-year statutes of limitations. 18 U.S.C. § 2520(e) (two years for ECPA claims); 18 U.S.C. § 1030(g) (two years for CFAA claims); 18 U.S.C. § 2707(f) (two years for SCA claims); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 624 (N.D. Cal. 2021) (two years limitation period for intrusion upon seclusion claims under Cal. Civ. Proc. Code § 335.1); *So v. Shin*, 212 Cal. App. 4th 652, 662 (2013) (two years for negligence claims under Cal. Civ. Proc. Code § 335.1); *McGowan v. Weinstein*, 505 F. Supp. 3d 1000, 1025 (C.D. Cal. 2020) (two years for negligent hiring claims under Cal. Civ. Proc. Code § 335.1). UCL and breach of contract claims have four-year statutes of limitations. Cal. Code of Civ. Proc. § 337(a) (four years for claims on written contracts); Cal. Bus. & Prof. Code § 17208 (four years for UCL claims). The statutes of limitations for unjust enrichment, promissory estoppel, and civil conspiracy are based on the underlying wrong. *Duke Gerstel Shearer, LLP v. Pursiano*, No. D060374, 2012 WL 4712102, at *5 (Cal. Ct. App. Oct. 4, 2012); *Newport Harbor Ventures, LLC v. Morris Cerullo World Evangelism*, 6 Cal. App. 5th 1207, 1224, n.5 212 Cal. Rptr. 3d 216, 229 (2016), *aff'd*, 4 Cal. 5th 637, 413 P.3d 650 (2018); *Maheu v. CBS, Inc.*, 201 Cal. App. 3d 662, 673, 247 Cal. Rptr. 304, 310 (Ct. App. 1988). If founded on a quasi-contract theory, the claim is two years. Cal. Civ. Proc. Code § 339(1). If founded on conversion, fraud, or mistake, it is three years. Cal. Civ. Code § 338(d); *Maheu*, 201 Cal. App. 3d at 673, 247 Cal. Rptr. 304, 310. If founded on a written contract, it is 4 years under Cal. Civ. Proc. Code § 337). Replevin has a three-year statute of limitations. Cal. Code of Civ. Proc. § 338.

discovery rule to apply, the plaintiff “must specifically plead facts to show (1) the time and manner of discovery and (2) the inability to have made earlier discovery despite reasonable diligence.” *Id.* at 808, 110 P.3d 914 (internal quotation marks omitted); *see McGowan v. Weinstein*, 505 F. Supp. 3d 1000, 1018–19 (C.D. Cal. 2020)

Al-Ahmed argues that November 2019 is the correct time for accrual for two reasons. First, he argues that he never received an email or in-app notice from Twitter in December 2015. Opp’n at 4. Thus, he had not discovered or had reason to discover any cause of action. *Id.* Second, even if he did receive such a notice, this notice did not include that these “state-sponsored actors” were located on Twitter’s premises, employed by Twitter, used Twitter’s resources, and acted at the direction or tacit permission of Twitter. *Id.* at 15. Thus, Al-Ahmed had no reason to know or believe that Twitter was complicit in, or, at the very least, negligent in its hiring, training, supervision and retention of the conduct of its employees until Alzabarah and Abouammo’s public indictment on November 19, 2019. Complaint at 15; Opp’n at 5-6. According to Al-Ahmed, this constitutes ignorance of the cause of action, as his causes of action for ECPA, CFAA, SCA, promissory estoppel, intrusion upon seclusion, negligent hiring, and negligence could not have accrued until he learned of Twitter’s involvement by virtue of the Twitter employees’ indictment. Under this construction, less than two years have passed between Al-Ahmed’s alleged discovery and the filing of the Complaint on October 13, 2021.

The first argument is unconvincing. In *Abdulaziz II*, the plaintiff had similarly argued that he did not receive Twitter’s notice and that the notice itself was insufficient. Nevertheless, the court dismissed the claim as time-barred. Although the Court did not explicitly discuss the November 2019 indictment of the two employees, it found that the December 2015 notice was sufficient notice to trigger the statute of limitations for the plaintiff’s negligent supervision and retention of its employees and negligence. The court explained:

The plaintiff does not dispute that Twitter sent the [December 2015] notices, but he disputes that he received them, contends they did not in any event warn him sufficiently of the breach, and asserts that he learned of the breach only on October 20, 2018 (rendering his lawsuit timely).

The December 2015 notice—that state actors potentially

compromised the plaintiff's Twitter account—was sufficient notice to trigger the statute of limitations. At that point, under California's discovery rule, the plaintiff "discover[ed], or has reason to discover, the cause of action."

Abdulaziz II, 2021 WL 633812, at *7 (internal citations omitted).

In *Abdulaziz I*, the court explained that the plaintiff did not meaningfully dispute that Twitter sent notices by simply asserting that he may not have received the notice when Twitter submitted its notification list. *See Abdulaziz I*, 2020 WL 6947929, at *7 ("The plaintiff does not meaningfully dispute that Twitter sent notices in December 2015. (Indeed, Twitter submitted its notification lists showing notice to the plaintiff.)"). Al-Ahmed's position here has similarly deficient. First, Al-Ahmed fails expressly to allege that he did not receive the notice in the Complaint, which only discusses the insufficiencies of the notice. Second, Al-Ahmed merely argues in his Opposition that he did not receive a notice despite carefully checking emails and that he never received an in-app notification -- which he cannot confirm because of his account suspension. Opp'n at 5. In any event, actual notice is not required for the statute of limitations to begin to run. *See Fox*, 35 Cal. 4th 797, 807 ("A plaintiff has reason to discover a cause of action when he or she has reason at least to suspect a factual basis for its elements."). As in *Abdulaziz I*, the fact that Al-Ahmed may not have received the notice does not prove that Twitter did not send notices. Like *Abdulaziz I*, Al-Ahmed does not dispute Twitter provided a notification list showing notice to Al-Ahmed.

Al-Ahmed's ignorance of the identity of the perpetrators (being Twitter employees) does not affect the statute of limitations, and ignorance of the cause of the action, which tolls the statute of limitations, also fails. As the Court noted in *Fox*, 35 Cal. 4th 797, 807, "failure to discover, or have reason to discover, the identity of the defendant does not postpone the accrual of a cause of action, whereas a like failure concerning the cause of action itself does." (Internal quotation marks and citations omitted.)

According to Al-Ahmed, the alleged lack of notice resulted in the ignorance of the cause of action, not the identity of the defendant. Opp'n at 5. However, when notified that his Twitter account had been hacked, he had notice that Twitter may have been responsible in some way, *e.g.*, by negligent failing to safeguard the security of his account. *See Roy-Condron v. Nazario*, No.

B263468, 2017 WL 432819, at *6 (Cal. Ct. App. Feb. 1, 2017); *see also Guerrero v. S. California Kaiser Permanente Med. Grp.*, No. B225999, 2011 WL 4375093, at *6 (Cal. Ct. App. Sept. 21, 2011) (plaintiff knew of the tortious conduct in 2005 even if he did not know the tortfeasor's employees; ignorance of the identity did not delay the running of the statute of limitations).

As the California Supreme Court stated, "the statute of limitations begins to run when the plaintiff suspects or should suspect that her injury was caused by wrongdoing, that someone has done something wrong to her." *Jolly v. Eli Lilly & Co.*, 44 Cal. 3d 1103, 1110 (1998). "The [a]ggrieved parties generally need not know the exact manner in which their injuries were effected, nor the identities of all parties who may have played a role therein." *Bernson v. Browning-Ferris Industries*, 7 Cal. 4th 926, 932 (1994)). The Ninth Circuit, quoting this language, also explained that it is the knowledge of the injury, not the identity of the defendant or the exact legal claim, that is required under California law:

[The plaintiff] knew about its injury in 2013 when it discovered the fraudulent accounts. It did not need to know the exact legal claim it could bring against a specific defendant. Rather, it was enough that it had knowledge of the injury that gave rise to the claim. Any liability it now claims against [the defendant] is derived from that injury in 2013.

Kyko Glob. Inc. v. Bhongir, No. 20-17526, 2021 WL 4958989, at *1 (9th Cir. Oct. 26, 2021).

Accordingly, the claims based on the unauthorized access of his account not saved by the discovery rule are barred under the statute of limitations.

The parties discuss the delayed discovery rule solely under California law. However, even if the federal discovery rule applies to the federal causes of action, there would be no meaningful difference because "[t]he federal accrual standard is essentially the same as the discovery rule." *Peterson v. Sutter Med. Found.*, No. 3:21-CV-04908-WHO, 2022 WL 316677, at *12 (N.D. Cal. Feb. 2, 2022) (citing *Lukovsky v. City & Cty. of San Francisco*, 535 F.3d 1044, 1048 (9th Cir. 2008)); *see also Mangum v. Action Collection Serv., Inc.*, 575 F.3d 935, 940 (9th Cir. 2009), *abrogated on other grounds by Rotkiske v. Klemm*, 140 S. Ct. 355, 205 L. Ed. 2d 291 (2019) ("[A] limitations period begins to run when the plaintiff knows or has reason to know of the injury which is the basis of the action." (citations omitted)). In a similar scenario, the Second Circuit

1 explained:

2 We pause to acknowledge that the statutes of limitations governing
3 claims under the CFAA and SCA, as we understand them, may have
4 troubling consequences in some situations. Even after a prospective
5 plaintiff discovers that an account has been hacked, the investigation
6 necessary to uncover the hacker's identity may be substantial. In
many cases, we suspect that it might take more than two years. But
it would appear that if a plaintiff cannot discover the hacker's
identity within two years of the date she discovers the damage or
violation, her claims under the CFAA and SCA will be untimely.

7 *Sewell v. Bernardin*, 795 F.3d 337, 342 (2d Cir. 2015); *see also Radcliff v. Radcliff*, No. CV 20-
8 3669, 2020 WL 7090687, at *5–7 (D.N.J. Dec. 4, 2020) (“[F]or statute of limitations purposes, a
9 CFAA claim starts to run when the plaintiff is aware of the alleged damage not when the plaintiff
10 learns exactly what has happened . . . [T]he main inquiry in determining when the statute of
11 limitation starts to accrue is when Plaintiff learned the integrity of her computer had been
12 compromised, even if the identity of the hacker was not known at the time.”).

13 Several cases illustrate why the statute of limitations began to run even if Al-Ahmed was
14 not aware of the precise roles of Twitter's employees. In *McGowan v. Weinstein*, the plaintiff was
15 sexually assaulted by Weinstein, who learned that she planned to expose him as her rapist through
16 a memoir in 2016. 505 F. Supp. 3d 1000, 1007 (C.D. Cal. 2020). A private intelligence agency,
17 Black Cube, was hired by Weinstein and Boies, and supervised by Bloom, to put the negative
18 campaign against Weinstein. *Id.* Although the plaintiff found out Weinstein, Boies, and Black
19 Cubes' involvement in 2017, she only learned about Bloom's role in September 2019 through an
20 article. *Id.* at 1009. Nevertheless, the court found that the applicable statute of limitations for the
21 negligent hiring and supervision claim against both Boies and Bloom began in 2017 despite her
22 late knowledge of Bloom's role because she failed to “plead facts to show . . . her inability to have
23 discovered the necessary information despite reasonable diligence.” *Id.* at 1025 (citing *Fox*, 35
24 Cal. 4th at 815). Like the plaintiff in *Weinstein* who alleged that she could not have discovered
25 Bloom's role until the 2019 article, Al-Ahmed similarly argues that he could not have discovered
26 Twitter's role until its employees' indictment. If anything, Al-Ahmed had a stronger basis for
27 investigating Twitter compared to the *Weinstein* plaintiff, as Twitter was not a third party
28 completely unknown and unrelated to the action because it was Twitter's data that had been

1 breached. In fact, Al-Ahmed argues in the Opposition that Twitter “negligently supervised nearly
2 everyone who had unneeded access,” not just Abouammo and Alzabarah, because “it was
3 reasonably foreseeable that someone in a company with 3,900 employees might do this.” Opp’n
4 at 21-22.

5 Similarly, in *Guerrero v. S. California Kaiser Permanente Med. Grp.*, a plaintiff sued an
6 employer for negligence and negligent hiring and supervision of their employee, who allegedly
7 stole the appellant's identity. No. B225999, 2011 WL 4375093, at *1 (Cal. Ct. App. Sept. 21,
8 2011). The plaintiff similarly argued that he had no proof of the employee’s identity until the
9 employee was criminally charged in 2006 and convicted in 2007. *Id.* at *3. Nevertheless, the
10 California Court of Appeals affirmed the trial court’s ruling that the claims were barred by the
11 statute of limitations because he knew of the tortious conduct in 2005 and that ignorance of the
12 identity did not delay the running of the statute of limitations. *Id.* at *6. The Court found that
13 there were sufficient facts at least for an inquiry notice to suspect Kaiser’s potential involvement.
14 Like *Weinstein* and *Guerrero*, Al-Ahmed was required to plead more to show that he was unable
15 to have made earlier discovery despite reasonable diligence. “[Conclusory allegations [do] not
16 withstand [dismissal].” *Fox*, 35 Cal. 4th 797, 808; *see also Hall v. Wal-Mart Stores, Inc.*, No. CV
17 H-15-3523, 2017 WL 462053, at *1 (S.D. Tex. Feb. 1, 2017) (finding that the lack of knowledge
18 that an unknown perpetrator was a Wal-Mart employee did not save the plaintiff’s claim from the
19 statute of limitations because had knowledge of the harm and “ignorance of the identity of the
20 party responsible for an injury does not affect the running of the limitations period”).

21 b. Fraudulent Concealment

22 Al-Ahmed next argues that Twitter deliberately and fraudulently concealed its involvement
23 to avoid liability, tolling the statute of limitations.³ *Id.* at 6 (“[T]he doctrine of fraudulent
24 concealment tolls the statute of limitations where a defendant, through deceptive conduct, has
25 caused a claim to grow stale.” (citing *Regents of the University of California v. Superior Court*, 20
26 Cal.4th 509, 533 (1999))).

27
28 ³ The correct term is equitable estoppel, not tolling. *See Vaca*, 198 Cal. App. 4th 737, 745, 129
Cal. Rptr. 3d 354, 360 (2011).

Under California’s fraudulent concealment doctrine, a defendant may be “estopped from profiting from its own misconduct” by asserting a statute of limitations defense “when a diligent plaintiff is unable to discover the defendant’s identity as a result of the defendant’s intentional efforts to conceal the identity of the defendant.” *Shively v. Bozanich*, 31 Cal. 4th 1230, 1249, 80 P.3d 676, 687 (2003); *Bernson*, 7 Cal.4th at 930, 30 Cal.Rptr.2d 440, 873 P.2d 613. “For a defendant to be equitably estopped from asserting a statute of limitations, the plaintiff must be directly prevented . . . from filing [a] suit on time.” *Vaca v. Wachovia Mortg. Corp.*, 198 Cal. App. 4th 737, 746, 129 Cal. Rptr. 3d 354, 360 (2011) (alteration in original) (quotation marks and citation omitted). *Bernson*’s standard “emphasiz[es] the burden on the plaintiff to demonstrate reasonable diligence, including the filing of a complaint against known defendants.” *Bernson*, 7 Cal.4th at 937, 30 Cal.Rptr.2d 440, 873 P.2d 613. “One factor which must be considered pertinent to the diligence inquiry is whether the filing of a timely Doe complaint would, as a practical matter, have facilitated the discovery of the defendant’s identity within the [statute of limitations].” *Id.* at 937, 30 Cal.Rptr.2d 440, 873 P.2d 613. Thus, “[w]here the identity of at least one defendant is known, for example, the plaintiff must avail himself of the opportunity to file a timely complaint naming Doe defendants and take discovery. However, where the facts are such that even discovery cannot pierce a defendant’s intentional efforts to conceal his identity, the plaintiff should not be penalized.” *Id.*

Al-Ahmed fails to allege any deceptive conduct by Twitter beyond the argument that Twitter’s notice did not specify that its own employees were involved. Although Al-Ahmed argues that “Twitter went through great lengths to conceal [its involvement and the identities of the perpetrators,]” this assertion is conclusory and unsupported by facts. Opp’n at 6. On the contrary, the December 2015 email and in-app notification provides sufficient notice of Al-Ahmed’s injury as well as Twitter’s failure to protect his account from data breaches by state-sponsored attacks. Al-Ahmed was aware of Twitter’s possible failure to implement policies and safeguards to prevent data breaches, even if he was unaware of the full extent of Twitter’s conduct via its employees who committed the breaches. He could have sought out the unknown hackers within the limitations period after filing a Doe complaint. *Id.*; accord *New Amsterdam Project*

1 *Mgmt. Humanitarian Found. v. Laughrin*, 400 F. App'x 250, 252 (9th Cir. 2010) (“Once the
2 plaintiff is aware of ‘a defendant,’ he can file a timely complaint naming Doe defendants and can
3 then utilize the available discovery tools to identify and serve any Doe defendants within the
4 applicable . . . statute of limitations.”). Discovery with Twitter likely would have led to the
5 discovery of the identities of the hackers. Therefore, this is not a case “where the facts are such
6 that even discovery cannot pierce a defendant’s intentional efforts to conceal his identity.”
7 *Bernson*, 7 Cal.4th at 937, 30 Cal.Rptr.2d 440, 873 P.2d 613. Accordingly, Al-Ahmed fails to
8 show any exercise of reasonable diligence, and the Court finds no fraudulent concealment by
9 Twitter.

10 3. The Continuous Accrual Doctrine

11 “[U]nder the theory of continuous accrual, a series of wrongs or injuries may be viewed as
12 each triggering its own limitations period, such that a suit for relief may be partially time-barred as
13 to older events but timely as to those within the applicable limitations period.” *Aryeh v. Canon*
14 *Bus. Solutions, Inc.*, 55 Cal. 4th 1185, 1192, 292 P.3d at 876 (2013). Continuous accrual applies
15 when there is a continuing or recurring obligation, such as monthly billing and payments, with
16 each month triggering a new limitations period. *Id.* at 1199, 292 P.3d at 880 (“When an obligation
17 or liability arises on a recurring basis, a cause of action accrues each time a wrongful act occurs,
18 triggering a new limitations period.”) (citation omitted); *see, e.g., Wolf v. Travolta*, 167 F. Supp.
19 3d 1077, 1104–05 (C.D. Cal. 2016) (citing *Tsemetzin v. Coast Fed. Sav. & Loan Assn.*, 57 Cal.
20 App. 4th 1334, 1344, 67 Cal. Rptr. 2d 726 (1997)); *Armstrong Petroleum Corp. v. Tri-Valley Oil*
21 *& Gas Co.*, 116 Cal. App. 4th 1375, 1388–89, 11 Cal. Rptr. 3d 412 (2004). Therefore, the theory
22 of continuous accrual “would permit [the plaintiff] to sue, but only for those discrete acts
23 occurring within the [relevant limitations period] immediately preceding the filing of [the
24 plaintiff’s] suit.” *Aryeh*, 55 Cal. 4th at 1199–200, 292 P.3d at 881.

25 Al-Ahmed argues that the continuous accrual doctrine makes portions of his claims timely.
26 Opp’n at 6. According to Al-Ahmed, Twitter breached its contractual obligations contained in its
27 TOS (express and implied), including its obligation to preserve Al-Ahmed’s confidential sources
28 and followers and its obligation to not unreasonably suspend his Arabic Twitter account in which

he has a reasonable expectation of privacy. Opp’n at 6–7. Al-Ahmed contends that Twitter continues to breach its TOS by keeping Al-Ahmed’s Twitter account suspended, which constitutes ongoing harms and liabilities that are “separate, recurring invasions of the same right [that] can each trigger their own statute of limitations.” *Id.* at 7–8 (citing *Aryeh* at 1198). Al-Ahmed lists Twitter’s ongoing wrongdoings as follows: 1) unlawfully accessing and disseminating his confidential sources, list of followers, and other proprietary electronic data and intellectual property, 2) suspending his Twitter account and withholding his sources and list of followers; 3) breaching contractual obligations contained in Twitter’s TOS; 4) deliberately, negligently, or recklessly employing operatives who continue to commit tortious acts against Al-Ahmed; 5) engaging in fraud such as making materially false statements regarding its obligations to and relationship with Al-Ahmed; and 6) violating Al-Ahmed’s First Amendment right to Free Speech and Freedom of Assembly. *Id.*

Al-Ahmed’s attempt to characterize the above acts as continuously recurring invasions fails. Rather, they are two distinct incidents: the unauthorized intrusion in 2015 and the suspension of Al-Ahmed’s Twitter account in 2018. The continued suspension of the account does not constitute a separate act, and “[w]ithout separate wrongful acts to trigger the statute of limitations, continuous accrual does not apply.” *Ryan v. Microsoft Corp.*, 147 F. Supp. 3d 868, 896-97 (N.D. Cal. 2015) (declining to apply rule where “alleged recurring injuries during the limitations period arose out of a single transaction that occurred before the limitations period”). Because both incidents are discrete and independent transactions, the continuous accrual doctrine does not apply. The statute of limitations on the suspension is separate and distinct from the limitations applicable to the hack.

For the foregoing reasons, all of Al-Ahmed’s claims against Twitter related to the unauthorized intrusion of his Twitter account are barred by the statute of limitations. All claims related to the 2018 account suspension are barred except any claims with a 4-year statute of limitations since this suit was not filed until October 2021. Accordingly, only the breach of contract claim, UCL claim, and the promissory estoppel claim based on the breach of contract, to

the extent that they are related to the 2018 account suspension, survive the time bar.⁴ However, for the reasons stated below, those claims are barred by the CDA Section 230(c)(1).

E. CDA Section 230(c)(1) and Al-Ahmed's Account Suspension-Related Claims

Twitter seeks immunity from Al-Ahmed's account-suspension-related claims under CDA Section 230(c)(1). Mot. at 15. Section 230(c), titled "Protection for "Good Samaritan" blocking and screening of offensive material, provides:

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
- (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

47 U.S.C.A. § 230.

In Section 230(b), Congress laid out the policies underlying this protection:

(b) Policy

It is the policy of the United States—

- (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
- (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
- (3) to encourage the development of technologies which maximize user control over what information is received by individuals,

⁴ Civil conspiracy and unjust enrichment claims are similarly based on the underlying wrong but are not premised on the breach of contract. See Complaint at 34–35; Opp'n at 35 ("Plaintiff's cause of action for restitution [is] based on quasi-contract/unjust enrichment is cognizable under California law as an alternative claim."). Accordingly, the 4-year statutes of limitations do not apply to these claims. The unjust enrichment claim is barred also because it alleges only the use and sale of Al-Ahmed's account, not the suspension of his account. See Complaint 25–26.

families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

47 U.S.C. § 230.

Section 230 “provides internet companies with immunity from certain claims in order to promote the continued development of the Internet and other interactive computer services.”

Lemmon v. Snap, Inc., 995 F.3d 1085, 1090–91 (9th Cir. 2021) (internal quotation marks and citations omitted). This immunity “shields from liability those individuals or entities that operate internet platforms, to the extent their platforms publish third-party content.” *Id.*

The Ninth Circuit explained:

Subsection (c)(1), by itself, shields from liability all publication decisions, whether to edit, to remove, or to post, with respect to content generated entirely by third parties. Subsection (c)(2), for its part, provides an additional shield from liability, but only for “any action voluntarily taken in good faith to restrict access to or availability of material that the provider ... considers to be obscene ... or otherwise objectionable.” § 230(c)(2)(A). Crucially, the persons who can take advantage of this liability shield are not merely those whom subsection (c)(1) already protects, but any provider of an interactive computer service. *See* § 230(c)(2). Thus, even those who cannot take advantage of subsection (c)(1), perhaps because they developed, even in part, the content at issue, *see Roommates*, 521 F.3d at 1162–63, can take advantage of subsection (c)(2) if they act to restrict access to the content because they consider it obscene or otherwise objectionable. Additionally, subsection (c)(2) also protects internet service providers from liability not for publishing or speaking, but rather for actions taken to restrict access to obscene or otherwise objectionable content.

Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (finding that a claim alleging defendant's failure to remove content was barred by Section 230(c)(1). As such, decisions to remove a user's posting is also considered a publishing decision which “involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content.” *Id.* at 1102.

To determine whether § 230(c)(1) applies, the Ninth Circuit set a three-prong test. *Id.* at 1096. Under this test, CDA immunity under § 230(c)(1) applies only if it is “(1) a provider or user

of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.” *Lemmon*, 995 F.3d at 1090–91.

The first prong is satisfied and undisputed by the parties. “Information content provider” is defined to include “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” 47 U.S.C. § 230(f)(3). “Twitter is a social media platform and provides the prototypical service entitling it to protections of [Section 230]” and “[e]very decision the Court has seen to consider the issue has treated Twitter as an interactive computer service provider, even at the motion to dismiss stage.” *Morton v. Twitter, Inc.*, No. CV 20-10434-GW-JEMX, 2021 WL 1181753, at *3 (C.D. Cal. Feb. 19, 2021) (internal quotation marks and citation omitted).

The second and third prongs are also satisfied. Al-Ahmed’s claims against Twitter are related to the suspension of his account. As discussed above, removal of posts and accounts of a user is generally considered as treating the information content provider as a publisher. *See Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1109 (9th Cir. 2009) (finding that the removal of social media content falls under Section 230(c)(1)); *see also King v. Facebook, Inc.*, No. 21-CV-04573-EMC, 2021 WL 5279823, at *1 (N.D. Cal. Nov. 12, 2021) (finding that claims relating to disabling of accounts fall under Section 230(c)(1)).

1. The Policies of Section 230

Al-Ahmed offers several arguments why Section 230 immunity should not apply. Al-Ahmed’s main argument is that Twitter’s attempt to invoke statutory immunity under Section 230(c) runs afoul of the policies and the fundamental purposes of the CDA. Opp’n at 11. First, Al-Ahmed argues that the Ninth Circuit has been dubious of large Internet companies seeking special privileges under the CDA. He quotes *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1164, n.15 (9th Cir.2008), stating, “The [CDA] was not meant to create a lawless no-man’s land on the Internet.” However, *Roommates* is inapposite because it concerned a housing website’s questionnaire that requires disclosure of the subscriber’s sex, sexual orientation, and status with children, which violated various housing laws. *Id.* at 1161.

1 The Ninth Circuit found that the posting of the questionnaires was the website’s own act and that
 2 the “CDA does not grant immunity for inducing third parties to express illegal preferences.” *Id.* at
 3 1165. The claim here does not involve Twitter posting as its own unlawful content.

4 Al-Ahmed also points to Justice Thomas’s concurrence in *Malwarebytes*, which expressed
 5 concerns that Section 230(c) under the Ninth Circuit’s expansive scope confers sweeping
 6 immunity that warrants revisitation in an appropriate case. Opp’n 9-10 (citing *Malwarebytes, Inc.*
 7 *v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 18, 208 L. Ed. 2d 197 (2020)). As this Court
 8 discussed in *King*, Justice Thomas’s concurrence does not constitute binding authority – it is a
 9 nonbinding concurrence. *King*, 2021 WL 5279823, at *10, *13.

10 Second, Al-Ahmed argues that immunity, applied to this case, would run contrary to the
 11 policy of protecting children from exposure to pornographic and obscene material, which he
 12 argues is the principal aim of Section 230. Opp’n at 11–12 (citing Section 230(b)(4)). According
 13 to Al-Ahmed, the suspension of his Twitter account, which bears no relationship to obscene
 14 materials, would render such policies illogical. *Id.* However, while it is true that Sections (b)(4)–
 15 (5) seek to enable filtering obscene materials and ensure their enforcement, the policies underlying
 16 Section 230 are not limited to obscene materials. For instance, Sections (b)(1)–(2) states: “[i]t is
 17 the policy of the United States – to promote the continued development of the Internet and other
 18 interactive computer services and other interactive media” and “preserve the vibrant and
 19 competitive free market that presently exists for the Internet . . . unfettered by Federal or State
 20 regulation.” 47 U.S.C. § 230(b).

21 In a similar vein, Al-Ahmed argues that because “the statute is intended to immunize an
 22 interactive service provider for engaging in tradition editorial functions in a public forum,” it
 23 “could never have been contemplated by the legislature to protect against or require the policing of
 24 private exchanges that are very much equivalent to private texts, phone calls or emails.” Opp’n at
 25 12–13. However, Al-Ahmed fails to cite any authority that limits protected editorial functions to
 26 material published in a public forum. Al-Ahmed cites a single Second Circuit case, *Force v.*
 27 *Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019), which merely notes that the word “publisher” is
 28 undefined by Section 230(c)(1). This case does not use the words “public forum.” *See id.* In fact,

a California court specifically discussed this issue and came to the opposite conclusion as follows:

Plaintiffs' other attempt to evade section 230(c)(1) is based on Twitter's Direct Messaging capabilities, which allow for the sending of private messages through the Twitter platform. Plaintiffs contend that publishing activity under section 230(c)(1) "necessarily involves the dissemination of information to the public" and thus does not encompass the transmission of private messages through Direct Messaging.

...

I am not persuaded that publishing activity under section 230(c)(1) does not extend to Twitter's Direct Messaging capabilities. As noted above, Congress enacted section 230(c)(1) in part to respond to a New York state court decision finding that an internet service provider could be held liable for defamation based on third-party content posted on its message boards. In defamation law, the term "publication" means "communication [of the defamatory matter] intentionally or by a negligent act to one other than the person defamed." The Fourth Circuit has held that an internet service provider covered by the "traditional definition" of publisher is protected by section 230(c)(1). And while the Ninth Circuit has declined to construe "the reach of section 230(c)(1) [as] fastened ... tightly to the nuances of defamation law," the court has also indicated that the statute's protections extend at least as far as the "treat[ment] [of] internet service providers as publishers ... for the purposes of defamation." Under this analysis, the private nature of Direct Messaging does not remove the transmission of such messages from the scope of publishing activity under section 230(c)(1).

Fields v. Twitter, Inc., 200 F. Supp. 3d 964, 974–75 (N.D. Cal. 2016) (citations omitted).

Third, Al-Ahmed argues that Twitter's suspension of his account suppresses the dissemination of free speech by "terminat[ing]/suspend[ing] the account of a prominent journalist democracy advocate against its most notable shareholders, the KSA[.]" which runs counter to the policy of "remov[ing] disincentives [to filter objectionable content.]" *Id.* at 13. Although Al-Ahmed's argument is not entirely clear, the CDA contemplates the ability of services like Twitter to employ filtering processes.

2. The Application of Section 230

Al-Ahmed next argues that a defendant who assists in the development of what made the content unlawful is not protected under Section 230. *Id.* (citing *Fed. Trade Comm'n v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016) ("A defendant . . . will not be held responsible unless it assisted in the development of what made the content unlawful."); *FTC v. Accusearch*

1 *Inc.*, 570 F.3d 1187, 1199 (10th Cir, 2009)); *Fair Hous. Council v. Roomates.com, LLC*, 521 F.3d
 2 1157, 1167–68 (holding the defendant liable when it had questionnaires “not merely...
 3 augmenting the content generally, but...materially contributing to its alleged unlawfulness”).
 4 However, the cases cited by Al-Ahmed are inapposite. *Roomates.com* is inapposite because the
 5 defendant, in that case, created and posted the questionnaire in question, thus inducing illegal acts
 6 of third parties. *Roomates.com, LLC*, 521 F.3d at 1165. Likewise, the defendant in *LeadClick*
 7 *Media* participated in the development of its affiliates’ deceptive websites, “materially
 8 contributing to [the content’s] alleged unlawfulness.” *LeadClick Media*, 838 F.3d at 176. Unlike
 9 *Roomates.com* and *LeadClick Media*, Twitter has not participated in the development of deceptive
 10 websites or required its subscribers to give information that would induce third parties to violate
 11 laws. Twitter seeks immunity for claims only in relation to the suspension of accounts of third
 12 party speakers.

13 Al-Ahmed next argues that Twitter cannot claim immunity under Section 230(c)(2)
 14 because it failed to demonstrate good faith. Opp’n at 14. However, this argument is irrelevant
 15 because Twitter seeks immunity under Section 230(c)(1), which does not have a good faith
 16 requirement, and does not seek immunity under Section 230(c)(2), which requires good faith.
 17 *Levitt v. Yelp! Inc.*, No. C-10-1321 EMC, 2011 WL 5079526, at *7 (N.D. Cal. Oct. 26, 2011),
 18 *aff’d*, 765 F.3d 1123 (9th Cir. 2014) (finding that while Section 230(c)(2) has a good-faith
 19 requirement, (c)(1) has no such requirement).

20 Some courts in other districts have declined to extend Section 230(c)(1) to cases in which
 21 the user brought claims based on their own content, not a third party’s, on the ground that it would
 22 render the good faith requirement of Section 230(c)(2) superfluous. *See, e.g., e-ventures*
 23 *Worldwide, LLC v. Google, Inc.*, No. 2:14-cv-646-FtM-PAM-CM, 2017 WL 2210029, at *3
 24 (M.D. Fl. Feb. 8, 2017). However, although a Florida court found the lack of this distinction to be
 25 problematic, it also noted that other courts, including those in this district, “have found that CDA
 26 immunity attaches when the content involved was created by the plaintiff.” *Id.* (citing *Sikhs for*
 27 *Just., Inc. v. Facebook, Inc.*, 697 F. App’x 526 (9th Cir. 2017) (affirming dismissal of the
 28 plaintiff’s claims based on Facebook blocking its page without an explanation under Section

1 230(c)(1)).

2 The California case cited by the Florida court, *Sikhs*, specifically addressed this issue. The
3 plaintiff had argued that there was no “third-party content” because it was the plaintiff who
4 created allegedly blocked Facebook page. *Sikhs for Just. “SFJ”, Inc. v. Facebook, Inc.*, 144 F.
5 Supp. 3d 1088, 1093 (N.D. Cal. 2015), *aff’d sub nom. Sikhs for Just.*, 697 F. App’x 526. The
6 court disagreed and analyzed the language of § 230(c)(1) as follows:

7 [I]t appears that Plaintiff denies the existence of “third-party
8 content” because there are only two parties in this litigation, Plaintiff
and Defendant. . . .

9 However, Plaintiff misunderstands the CDA. By its terms, the CDA
10 precludes publisher liability against an interactive computer service
for content created by “another information content provider.” 47
11 U.S.C. § 230(c)(1). An “information content provider” is defined as
“any person or entity that is responsible, in whole or in part, for the
12 creation or development of information provided through the
Internet or any other interactive computer service.” *Id.* § 230(f)(3).
13 . . .

14 [T]he CDA immunizes an interactive computer service provider that
“passively displays content that is created entirely by third parties,”
15 but not an interactive computer service provider that acts as an
information content provider by creating or developing the content
at issue. *Roommates*, 521 F.3d at 1162. Put another way, “third-
16 party content” is used to refer to content created entirely by
individuals or entities other than the interactive computer service
17 provider. *See id.* By contrast, the number of parties in a given
litigation is irrelevant to CDA immunity.

18 In this case, the complaint asserts that the . . . Page was provided by
19 Plaintiff, not Defendant. Compl. at 1, 7. . . . By contrast, the
complaint nowhere alleges that Defendant provided, created, or
20 developed any portion or content of the . . . Page. . . . Instead,
Plaintiff argues that “the content belongs to [Plaintiff] and was put
21 on Defendant's online platform.” Opp. at 3. Accordingly, only
Plaintiff, not Defendant, acts as an information content provider in
22 this case. As a result, the . . . Page, which was created entirely by
Plaintiff, is “information provided by another information content
23 provider” within the meaning of § 230. *See Roommates*, 521 F.3d at
1162.

24
25 *Id.* Other courts in this district and the Ninth Circuit have similarly applied Section 230(c)(1) to
26 claims where a user’s own content was removed. *See also Riggs v. MySpace, Inc.*, 444 F. App’x
27 986, 987 (9th Cir. 2011) (affirming dismissal under Section 230(c)(1) claims based on the removal
28 of the plaintiff’s user profile, noting that “[a]ny activity that can be boiled down to deciding

whether to exclude material that third parties seek to post online is perforce immune under section 230” (quoting *Roommates*, 521 F.3d at 1164, n.15, 1170–71; *see also* *Murphy v. Twitter, Inc.*, 60 Cal. App. 5th 12, 27, 274 Cal. Rptr. 3d 360, 370 (2021). As such, the Court follows the approach taken by others this district and applies Section 230(c)(1) to allegations of removal of a user’s content. Because Section 230(c)(1) applies here, and Twitter is not required to demonstrate good faith.

As the California Court of Appeal noted in *Murphy*, 60 Cal. App. at 27, 274 Cal. Rptr. 3d at 370, “[c]ourts have routinely rejected a wide variety of civil claims like [the plaintiff’s] that seek to hold interactive computer services liable for removing or blocking content or suspending or deleting accounts (or failing to do so) on the grounds they are barred by the CDA.” The court found it was proper to dismiss plaintiff’s claims of breach of contract, promissory estoppel, and violation of the UCL claims as barred under section 230(c)(1)).

This Court’s decision in *King v. Facebook* closely mirrors this case. In *King*, the plaintiff had a personal account with about 1,000 friends who shared both political and nonpolitical information. *King*, 2021 WL 5279823, at *1. The account was disabled by Facebook. This Court held that Facebook had CDA immunity under Section 230(c)(1) to the extent his contract and implied covenant claims were based on Facebook’s disabling of the plaintiff’s account. This Court held, however, that CDA immunity did not apply to the extent that the claim was based on Facebook’s failure to provide an explanation for the disabling of the account. *Id.* at 13. The court reasoned that this specific claim was tied to an implied promise to explain its decision that does not depend on Facebook’s status as a publisher. *Id.* (the terms of service stated: “[wh]ere we take such action [account suspension or termination] we’ll let you know and explain any options you have to request a review”). *Id.* at *8.

Accordingly, Twitter’s immunity extends to all of Al-Ahmed’s suspension-based claims, but not his breach of contract claim based on Twitter’s failure to provide adequate justification for the suspension and to adequately or meaningfully address and consider his appeal from the suspension of his account. Nevertheless, this claim fails because Al-Ahmed fails to articulate any reason why a failure to provide a justification for the suspension constitutes a breach of contract.

Unlike Facebook's terms of service in *King*, Al-Ahmed's Complaint does not point to, and Twitter's TOS does not seem to include or imply a similar provision that would constitute a promise to address any suspensions and appeal them. Therefore, this remaining claim is also dismissed.

V. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Twitter's motion to dismiss in its entirety. Al-Ahmed seeks leave to amend the Complaint to allege a Lanham Act claim that falls within the scope of the CDA's intellectual property exception. *See* 47 U.S.C. § 230(e)(2) ("Nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property."); *see Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1053 (9th Cir. 2019) (discussing that § 230(e)(2)'s exception may apply to Lanham claims involving intellectual property).⁵ The First Amended Complaint, if any, is due within thirty (30) days of the date of this order.

This order disposes of Docket No. 30.

IT IS SO ORDERED.

Dated: May 20, 2022


EDWARD M. CHEN
United States District Judge

⁵ Courts have found that some Lanham Act claims fall within the scope of the CDA's intellectual property exception. *Id.*; 47 U.S.C. § 230(e)(2). ("Nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property.").